

1 CLAIMS

2 What is claimed is:

3 1. A method to reduce a search space for determining viable cellular  
4 automata based random number generators (CA-based RNGs), comprising:

5 counting number of 1s and 0s of outputs of a truth table for a candidate CA-  
6 based RNG;

7 counting number of 1s and 0s of inputs of said truth table for said candidate  
8 CA-based RNG; and

9 accepting or rejecting said candidate CA-based RNG based on results of said  
10 counting steps.

11

12 2. The method of claim 1, wherein in said step of accepting or rejecting  
13 said candidate CA-based RNG comprises:

14 accepting said candidate CA-based RNG in response to all of the following  
15 conditions being met:

16 a difference of counts of 1s and 0s in said outputs of said truth table is  
17 less than or equal to a predetermined output difference threshold;

18 a difference of counts of 1s and 0s in said inputs of said truth table  
19 generating 1s for output is less than or equal to a predetermined 1s input  
20 difference threshold; and

21 a difference of counts of 1s and 0s in said inputs of said truth table  
22 generating 0s for output is less than or equal to a predetermined 0s input  
23 difference threshold.

24

1           3.     The method of claim 2, wherein at least one of said predetermined  
2     output difference threshold, predetermined 0s input difference threshold, and  
3     predetermined 1s input difference threshold is zero.

4  
5           4.     The method of claim 1, wherein in said step of accepting or rejecting  
6     said candidate CA-based RNG comprises:

7           rejecting said candidate CA-based RNG in response to at least one of the  
8     following conditions not being met:

9                     a difference of counts of 1s and 0s in said outputs of said truth table is  
10           less than or equal to a predetermined output difference threshold;

11                    a difference of counts of 1s and 0s in said inputs of said truth table  
12           generating 1s for output is less than or equal to a predetermined 1s input  
13           difference threshold; and

14                    a difference of counts of 1s and 0s in said inputs of said truth table  
15           generating 0s for output is less than or equal to a predetermined 0s input  
16           difference threshold.

17  
18           5.     The method of claim 4, wherein at least one of said predetermined  
19     output difference threshold, predetermined 0s input difference threshold, and  
20     predetermined 1s input difference threshold is zero.

21  
22           6.     A system to reduce a search space for determining viable cellular  
23     automata based random number generator (CA-based RNGs), comprising:

24           a truth-table-counting-module counting number of 1s and 0s of outputs of a  
25     truth table for a candidate CA-based RNG, said truth-table-counting module also

1 counting number of 1s and 0s of inputs of said truth table for said candidate CA-based  
2 RNG; and  
3 a prescreening-module accepting or rejecting said candidate CA-based RNG  
4 based on an output or outputs of said truth-table-counting module.  
5

6 7. The system of claim 6, wherein said truth-table-counting-module  
7 comprises:

8 an output-counting-module counting number of 1s and 0s of said outputs of  
9 said truth table for said candidate CA-based RNG; and

10 an input-counting-module counting number of 1s and 0s of said inputs of said  
11 truth table for said candidate CA-based RNG.  
12

13 8. The system of claim 6, wherein said prescreening-module accepts said  
14 candidate CA-based RNG accepts in response to all of the following conditions being  
15 met:

16 a difference of counts of 1s and 0s in said outputs of said truth table is less  
17 than or equal to a predetermined output difference threshold;

18 a difference of counts of 1s and 0s in said inputs of said truth table generating  
19 1s for output is less than or equal to a predetermined 1s input difference threshold;  
20 and

21 a difference of counts of 1s and 0s in said inputs of said truth table generating  
22 0s for output is less than or equal to a predetermined 0s input difference threshold.  
23

1           9.     The system of claim 8, wherein at least one of said predetermined  
2     output difference threshold, predetermined 0s input difference threshold, and  
3     predetermined 1s input difference threshold is zero.

4  
5           10.    The system of claim 6, wherein in said prescreening-module accepts  
6     said candidate CA-based RNG rejects in response to at least one of the following  
7     conditions not being met:

8           a difference of counts of 1s and 0s in said outputs of said truth table is less  
9     than or equal to a predetermined output difference threshold;

10          a difference of counts of 1s and 0s in said inputs of said truth table generating  
11     1s for output is less than or equal to a predetermined 1s input difference threshold;  
12     and

13          a difference of counts of 1s and 0s in said inputs of said truth table generating  
14     0s for output is less than or equal to a predetermined 0s input difference threshold.

15

16          11.    The system of claim 10, wherein at least one of said predetermined  
17     output difference threshold, predetermined 0s input difference threshold, and  
18     predetermined 1s input difference threshold is zero.

19

20          12.    A computer readable medium on which is embedded computer  
21     software comprising a set of instructions for performing a method to reduce a search  
22     space for determining viable cellular automata based random number generator (CA-  
23     based RNGs), said method comprising:

24          counting number of 1s and 0s of outputs of a truth table for a candidate CA-  
25     based RNG;

1 counting number of 1s and 0s of inputs of said truth table for said candidate  
2 CA-based RNG; and  
3 accepting or rejecting said candidate CA-based RNG based on results of said  
4 counting steps.

5

6 13. The computer readable medium of claim 12, wherein in said method  
7 (200), said step of accepting or rejecting said candidate CA-based RNG comprises:  
8 accepting said candidate CA-based RNG in response to all of the following  
9 conditions being met:

10 a difference of counts of 1s and 0s in said outputs of said truth table is  
11 less than or equal to a predetermined output difference threshold;

12 a difference of counts of 1s and 0s in said inputs of said truth table  
13 generating 1s for output is less than or equal to a predetermined 1s input  
14 difference threshold; and

15 a difference of counts of 1s and 0s in said inputs of said truth table  
16 generating 0s for output is less than or equal to a predetermined 0s input  
17 difference threshold.

18

19 14. The computer readable medium of claim 13, wherein at least one of  
20 said predetermined output difference threshold, predetermined 0s input difference  
21 threshold, and predetermined 1s input difference threshold is zero.

22

1           15.     The computer readable medium of claim 12, wherein in said method,  
2     said step of accepting or rejecting said candidate CA-based RNG comprises:

3           rejecting said candidate CA-based RNG in response to at least one of the  
4     following conditions not being met:

5                     a difference of counts of 1s and 0s in said outputs of said truth table is  
6     less than or equal to a predetermined output difference threshold;

7                     a difference of counts of 1s and 0s in said inputs of said truth table  
8     generating 1s for output is less than or equal to a predetermined 1s input  
9     difference threshold; and

10                    a difference of counts of 1s and 0s in said inputs of said truth table  
11     generating 0s for output is less than or equal to a predetermined 0s input  
12     difference threshold.

13

14           16.     The computer readable medium of claim 15, wherein at least one of  
15     said predetermined output difference threshold, predetermined 0s input difference  
16     threshold, and predetermined 1s input difference threshold is zero.